PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32 | A2 | (11) International Publication Number: WO 99/62222

(43) International Publication Date: 2 December 1999 (02.12.99)

(21) International Application Number: PCT/SE99/00814

(22) International Filing Date: 12 May 1999 (12.05.99)

(30) Priority Data:
9801871-6 27 May 1998 (27.05.98) SE

(71) Applicant (*for all designated States except US*): TELIA AB (publ) [SE/SE]; Mårbackagatan 11, S-123 86 Farsta (SE).

(72) Inventors; and
(75) Inventors/Applicants (*for US only*): GUSTAVSSON, Per [SE/SE]; Kaplanst 2, S-240 13 Genarp (SE). LUNDGREN, Staffan [SE/SE]; Dag Hammarsköldsv 5 J, S-224 64 Lund (SE). MÅRTENSSON, Mattias [SE/SE]; Majbaggevägen 7, S-247 35 S. Sandby (SE). ÅHLIN, Eskil [SE/SE]; Östra Vallgatan 49, S-223 61 Lund (SE).

(74) Agent: PRAGSTEN, Rolf; Telia Research AB, Vitsandsgatan 9, S-123 86 Farsta (SE).

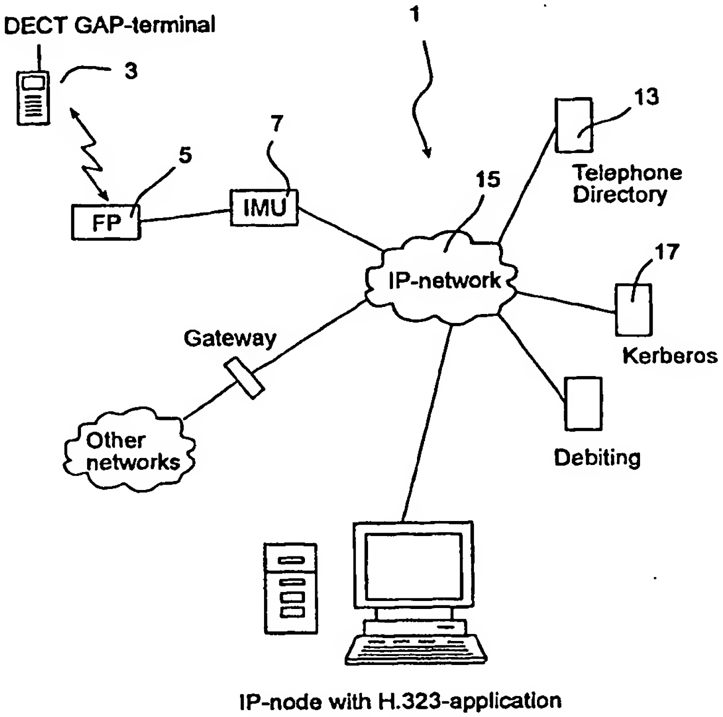
(81) Designated States: EE, JP, LT, LV, NO, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD FOR SAFE TELEPHONY WITH MOBILITY IN A TELE AND DATA COMMUNICATIONS SYSTEM WHICH INCLUDES AN IP-NETWORK

(57) Abstract

The invention relates to a method for safe telephony with mobility in a tele and data communications system (1) which includes an IP-network (15), at which the telephony is executed with mobile units and at which the method for each mobile unit includes the steps: to create a unique identity code and store it in the unit; to, at the switching on of the unit, at least at switching it on in a home domain, transmit the identity code to a mobility manager (9); to, via the IP-network, establish contact between the mobility manager and an initiating database (13) for transmission of initiating information for Internet communication from the initiating data base to the mobility manager, which step includes to, by utilisation of the identity code, authenticate the mobility manager for access to the initiating data base, and to encrypt the initiating information at the transmission; and to, by means of the initiating information, start a proxy (11) which represents the unit towards the Internet.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD FOR SAFE TELEPHONY WITH MOBILITY IN A TELE AND DATA COMMUNICATIONS SYSTEM WHICH INCLUDES AN IP-NETWORK

TECHNICAL FIELD

The present invention relates to a method for safe telephony with mobility in a tele and data communications system which includes an IP-network.

BACKGROUND OF THE TECHNOLOGY

In a data and telecommunications system which offers a user IP-telephony with mobility, the integrity of the Internet-traffic must be taken into consideration. This means for instance that the network operator can debit services to right account and that there is no risk for unauthorised utilisation.

For that reason there is a great need of well functioning security systems which as far as possible guarantee a correct and safe identification of a user. This is not least of importance for a correct debiting. Further, for example, an unauthorised person shall not be in a position to forward telephone calls and shall not be in a position to take part in the communication between two users of the system. Communication channels in the system for that reason must be encrypted and authenticated. This, in its turn, creates a need for common keys.

If all participants in the system would exchange and store each other´s keys, this would involve a security risk. Besides it would impair the scalability of the system.

A known solution of the managing of keys is called Kerberos©. This known solution provides a central distribution of keys and is intended for users of services in networks. Kerberos® attends to that the user can confirm his/her identity to a given service without risk that anybody is tapping the transmission in order to in a later stage unduly borrow the user´s identity. In this known solution an authentication is performed in two steps. In the first step one issues an authentication service (AS), a so called TGS-ticket in exchange for a person proving that he/she is the person he/she gives himself/herself out to be.

The user identification is made by the user initially once and for all registers himself/herself manually and receives a password from Kerberos®. The password is stored centrally. When the user then wants to utilise services in the network he/she orders the TGS-ticket with his/her user identity as identification. The TGS-ticket includes i.a. a TGS-session key, the name of the service (i.e. TGS), a time stamp and period of validity. In return from the TGS the user receives the TGS-ticket encrypted by TGS password and a copy of the TGS-session key encrypted by the user´s password. By that, only the true user can decrypt and utilise the information. In this way the password is never transmitted freely over the network.

The TGS-ticket is valid as access to a ticket issuing service (TGS). In the second step, the user for that reason turns to TGS to get service tickets to other services. In this step the user transmits the TGS-ticket encrypted by TGS password and the name of the service which is asked for to TGS. TGS returns a ticket to the service encrypted by the password of the service and a copy of a service session key encrypted by the TGS-session key. For each new service the user wants to utilise he/she in the same way turns to said TGS and encloses his/her TGS-ticket in the transmission.

This known method has several advantages. The user need only give his/her password once per working period. Only registered users can utilise the system because the user has to authenticate himself/herself at AT before he/she receives a ticket for a service. Services know that the user is authentic and not anyone who has copied the original message, because only the authentic sender knows the session key and is in a position to decode the traffic. The user also knows that a service is genuine because the session key in the ticket is encrypted by the key of the service. Only the genuine service consequently can decode the session key. Besides the user is always waiting for answer and consequently can be sure that the service is genuine.

The method according to Kerberos®, however, is not directly applicable on IP-telephony with mobility, such as a system with DECT-telephones which have access to an IP-network. For that reason there exists a need for a security solution for such telephony.

SUMMARY FO THE INVENTION

The aim of the present invention consequently is to create a security solution for IP-telephony with mobility.

The object is achieved by a method for safe communication according to the invention as it is defined in patent claim 1 of the enclosed patent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, embodiments of the method according to the invention will be described in detail with reference to the enclosed drawings, where:

Figure 1 diagrammatically shows a tele and data communications system in which an embodiment of the method is implemented; and

Figure 2 diagrammatically shows a part of the system in Figure 1 in detail.

DETAILED DESCRIPTION OF EMBODIMENTS

Below, a preferred embodiment of the method according to the invention will be described, at which it is exemplified applied in a tele and data communications system which includes wireless telephones in form of DECT-telephones and which is shown in Figure 1. The method according to the invention is especially suited for such systems.

In each DECT-telephone 3 an identity code (ID-code) is stored which is created in such a way that it is unique, preferably globally unique. When the DECT-telephone 3 is in its home domain, i.e. a DECT-domain, and is switched on, the ID-code is transmitted to the base station 5 of the domain. From there the ID-code is forwarded to a mobility manager, here a so called proxy manager 9, see Figure 2, which is arranged in an IP-managing unit (IMU) 7. The proxy manager 9 starts for each DECT-telephone 3 a proxy 11, i.e. en proxy which represents the DECT-telephone 3 towards the Internet, or any other IP-network. The proxy manager 9, however requires a certain initiating information to be able to start a proxy 11. The information is collected from a specific initiating database 13, which here is called telephone directory. The telephone directory is reached via the IP-network 15. In order to have the information transmitted in a safe way, the above mentioned described known method called Kerberos® is utilised, and which i.a. is implemented on a server 17, which handles the central distribution of keys. The information includes IP-address, the subscriber´s user name, and a key for mobile IP.

In this situation the proxy manager 9 is user and the telephone directory 13 the service which shall be used. For the proxy manager 9 to receive the information, it consequently must authenticate itself to the AS-part of the server 17 to get a TGS-ticket, and then utilises the identity code as user identity, and then by transmitting the TGS-ticket to the TGS-part of the server 17 receive a service ticket to the telephone directory. The information is transmitted well encrypted from the telephone directory 13 to the proxy manager 9, as has been described above. The proxy manager 9 then starts a proxy 11 with the information as input data.

The proxy 11 now has the function of a mobile node. If it should be in a foreign network it will make use of a mobile IP to attend to that traffic which is intended for it is routed to right address. Within mobile IP authentication is of outmost importance because unauthorised persons without authentication might change the traffic in the system as they please, or fraudulently give themselves out as another persons than they are. This authentication is made by means of an encryption algorithm and a secret key which is shared by the mobile node, i.e. the proxy 11, and the mobility manager in its home network. The secret key is the above mentioned key for mobile IP which the proxy manager 9 receivers from the database 13.

When the subscriber wants to utilise any of the services which the network operator offers, for instance make a call, both the subscriber and the operator are interested in that the debiting for the utilisation will be correct. The proxy 11 then contacts a debiting service to charge right account with right sum. This communication is also made by means of Kerberos®.

The proxy 11 is preferably compatible with the ITU-standard H.323, which can be utilised according to the following. At the communication between two subscribers, the receiver collects a session key from Kerberos® and establishes a safe and authenticated channel. After that H.323 follows on. The speech is accordingly transmitted encrypted in order that it shall not be possible to tap. At the same time participants, which are not authorised subscribers in the system, are prevented, by the authentication, from making free calls.

Above, a preferred embodiment of the method according to the invention has been described. This shall only be regarded as an example of how the invention can be implemented. A lot of modifications are possible within the frame of the invention as it is defined in the patent claims. Below follows some examples of such modifications.

Above, the method has been described for IP-telephony with DECT-telephones. It is also applicable for other types of mobile IP-telephony. One example is a computer which is moved between different access points.

The above described key distribution method Kerberos® can be exchanged for another equivalent method which implies equivalent good authentication and encryption.

PATENT CLAIMS

1. Method for safe telephony with mobility in a tele and data communications system (1) which includes an IP-network (15), at which the telephony is executed by mobile units, and at which the method for each mobile unit is characterised in the steps:

- to create a unique identity code and store it in the unit;
- to, when the unit is switched on, at least when it is switched on in a home domain, transmit the identity code to a mobility manager (9);
- to, via the IP-network, establish contact between the mobility manager and an initiating database (13) for transmission of initiating information for Internet communication from the initiation database to the mobility manager, which step includes to, by utilisation of the identity code, authenticate the mobility manager for access to the initiation database, and to encrypt the initiation information at the transmission; and
- to, by means of the initiating information, start a proxy (11) which represents the unit towards Internet.

2. Method according to patent claim 1, characterised in that said proxy for access to services in the communications system initially via the IP-network by means of in the initiating information included data authenticates itself to a server which centrally manages keys, at which the proxy from a part of the server receives a TGS-ticket and after that, by providing the TGS-ticket, via a TGS-part of said server receives service tickets for different services, at which each service ticket includes one for the service in question specific session key.

3. Method according to patent claim 1 or 2,

characterised in that in the data base store initiating information which for each user includes IP-address and key for mobile IP.

4. Method according to any of the preceding patent claims, characterised in that the step to, when the unit is switched on, at least when it is switched on in a home domain, transmit the identity code to a mobility manager, when the unit is a DECT-telephone, includes to transmit the identity code from the telephone to a base station (5) in the home domain, and to forward the identity code from the base station to the mobility manager.

5. Method according to any of the precedent patent claims, characterised in that the proxy, when it is in a foreign network, makes use of a mobile IP to attend to that traffic which is intended for it, is routed to right address.

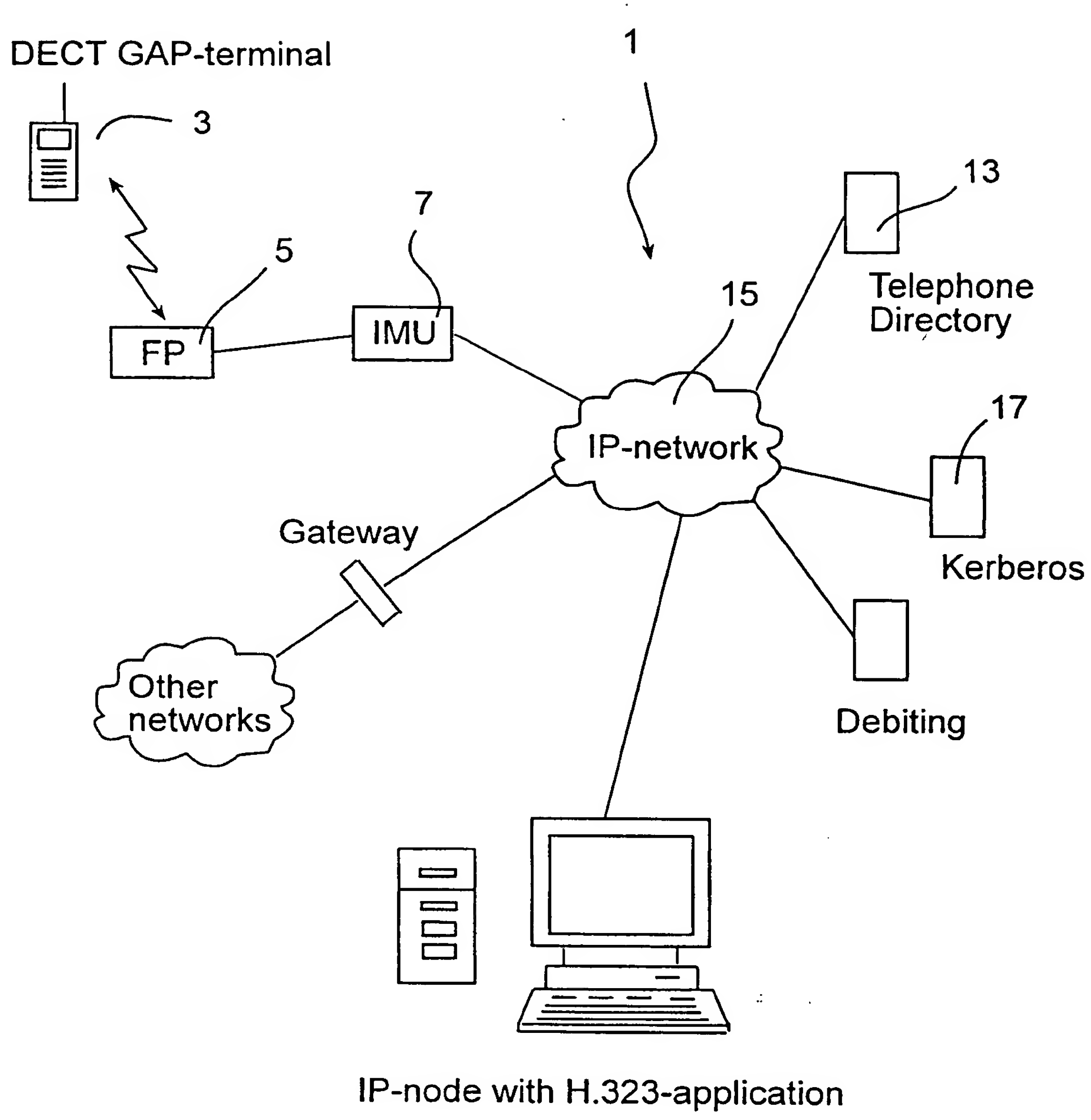

DECT GAP-terminal
1
3
13
7
5
Telephone Directory
15
FP
IMU
17
IP-network
Gateway
Kerberos
Other networks
Debiting
IP-node with H.323-application

Figure 1

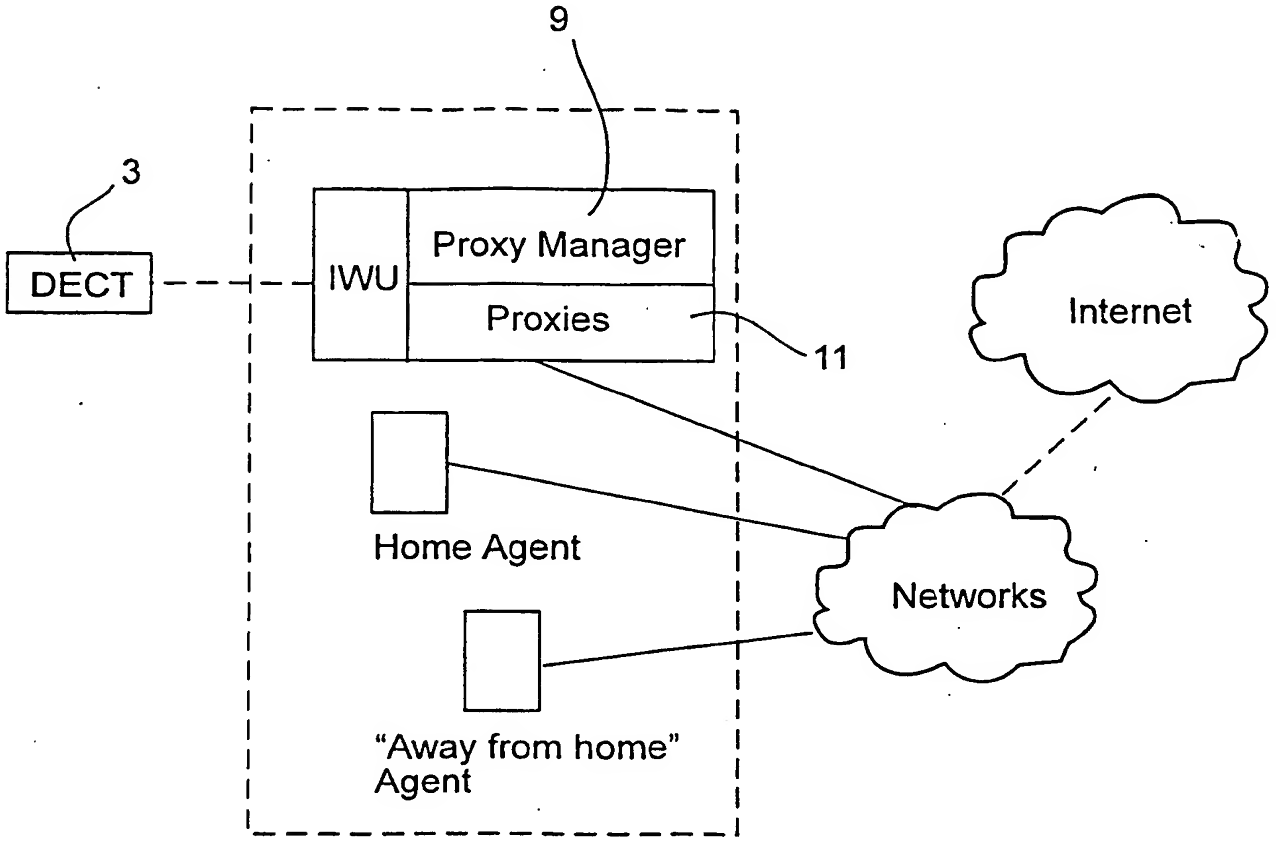

9
3
DECT
IWU
Proxy Manager
Proxies
11
Internet
Home Agent
Networks
"Away from home" Agent

Figure 2